UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,167	06/24/2003	Christian Gehrmann	8196-14XX	9436

20792 7590 03/06/2007
MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/602,167	**Applicant(s)** GEHRMANN, CHRISTIAN	
	Examiner Thanhnga B. Truong	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 June 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 June 2003* is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Thanhnga B. Tr

AU2135

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *2/14/03; 4/5/03*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on June 24, 2003. Claims 1-12 are pending. At this time, claims 1-12 are rejected.

Information Disclosure Statement

2. The information disclosure statement (IDS) filed on February 17, 2004 and April 5, 2004. The submissions are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 10 and 11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

a. *Referring to claims 10-11:*

Claim 10 and 11 recite "a computer program product configured to process a message to determine a tag value from the message and from a key according to a message authentication code." The claim is clearly a software program and it is non-statutory as not being tangibly embodied in a manner so as to be executable. Furthermore, applicant has pointed out in the specification (see lines 6-14 of page 5) "**the following may be implemented in software and carried out in a data processing system or other processing means caused by the execution of computer-executable instructions. The instructions may be program code means loaded in a memory, such as a RAM, from a storage medium or from another computer via a computer network. Alternatively, the described features may be implemented by hardwired circuitry instead of software or in combination with software**", which clearly including intangible media such as signals, carrier waves, transmissions, optical waves, transmission media or other media incapable of being touched or perceived absent the tangible medium through which they are conveyed. Therefore, claims 10 and 11 recite a non-statutory subject matter.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-5, 7-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Graveman (US 6,851,052 B1), and further in view of Lerner (US 6,718,503 B1).

a. <u>Referring to claim 1:</u>

i. Graveman teaches a method of processing a message to determine a tag value from the message and from a key according to a message authentication code (column 5, lines 13-30 of Graveman), the method comprising:

(1) selecting one of a plurality of symbols (e.g., vectors), the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and determining the tag value to be the selected symbol **(column 5, lines 13-40; column 6, line 64 through column 7, line 19; column 8, lines 31-35 of Graveman)**.

ii. Although Graveman teaches the technique to process message authentication code using initial vectors (which is the symbols of the codeword), Graveman is silent on the capability of showing the details of forming a codeword. On the other hand, Lerner teaches how a codeword is forming **(see Figure 1 and more details in column 2, lines 28-40 of Lerner)**.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Graveman (if indeed is not inherently) with the teaching of Lerner to authenticating the source and integrity of transmitted or stored information **(column 1, lines 24-25 of Graveman)**.

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Graveman (if indeed is not inherently) with the teaching of Lerner to provide absolute authentication of the source or origin of a received message and permits verifying approximate integrity between the original message and the received message **(column 1, lines 28-31 of Graveman)**.

b. *Referring to claim 2:*

i. Graveman further teaches:

(1) wherein the data item derived from the message consists of said message **(column 8, lines 29-48 of Graveman)**.

c. *Referring to claim 3:*

i. Graveman further teaches:

(1) further comprising determining said data item to be a hash value of a one-way hash function calculated from the message **(column 1, lines 42-45 and line 55 through column 2, line 7 of Graveman)**.

d. *Referring to claim 4:*

i. The combination of the teaching between Graveman and Lerner teaches the length of the key **(column 6, lines 44-48 of Graveman),** and Lerner further teaches:

(1) wherein the key is short enough to be communicated via a user interaction **(column 3, lines 47-56; column 8, lines 9-11 of Lerner)**.

e. *Referring to claim 5:*

i. The combination of the teaching between Graveman and Lerner teaches the type of error correction code, wherein Reed-Solomon is one kind of error correcting code **(column 5, lines 37-40 of Graveman),** and Lerner further teaches:

(1) wherein the error correcting code is a Reed-Solomon code and wherein the tag value is determined by evaluating a Reed-Solomon encoding polynomial at a point determined by the key **(column 1, lines 40-41 of Graveman)**.

f. *Referring to claim 7:*

i. Graveman further teaches:

(1) further comprising communicating at least a contribution to the message from a sender to a receiver via a first communications channel **(column 5, lines 36-40 of Graveman)**; and communicating the tag value and/or the key from the sender to the receiver via a second communications channel different from the first communications channel **(column 10, lines 16-26 of Graveman)**.

g. *Referring to claim 8:*

i. Graveman further teaches:

(1) wherein the second communications channel includes a user interaction **(column 2, lines 11-16 of Graveman)**.

h. *Referring to claims 9 and 12:*

i. These claims consist a communications device for communicating data messages, the communications device to implement claim 1, thus they are rejected with the same rationale applied against claim 1 above.

i. *Referring to claims 10 and 11:*

i. These claims consist a computer program product configured to process a message to determine a tag value from the message and from a key according to a message authentication code, the computer program product to implement claim 1, thus they are rejected with the same rationale applied against claim 1 above.

7. Claims 5-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Graveman (US 6,851,052 B1), in view of Lerner (US 6,718,503 B1), and further in view of Shokrollahi (US 6,631,172).

a. *Referring to claims 5 and 6:*

i. The combination of the teaching between Graveman and Lerner teaches the type of error correction code, wherein Reed-Solomon is one kind of error correcting code which defines in terms of finite field. However they are silent on the capability to show the tag value is an element in a finite field **(column 5, lines 37-40 of Graveman).** On the other hand, Shokrollahi teaches this limitation (as shown in column 1, lines 19-35 of Shokrollahi).

ii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Graveman-modified (if indeed is not inherently) with the teaching of Shokrollahi to authenticating the source and integrity of transmitted or stored information **(column 1, lines 24-25 of Graveman).**

iii. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Graveman-modified (if indeed is not inherently) with the teaching of Shokrollahi to provide absolute authentication of the source or origin of a received message and permits verifying approximate integrity between the original message and the received message **(column 1, lines 28-31 of Graveman).**

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Corrington et al (US 4,688,250) discloses messages sent from an earth station to a satellite by a command link are authenticated within the satellite before being executed. Authentication is accomplished by comparing a codeword appended to the message to a codeword generated within the satellite. This codeword is a cryptographic function of the message data and a secret operating key (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Thanhnga B. Truong
AU2135

TBT
February 28, 2007